PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-118042
(43)Date of publication of application : 27.04.2001

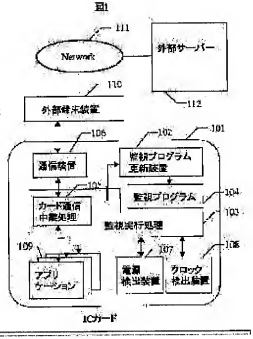
(51)Int.Cl. G06K 19/073
G06F 12/14
G06K 17/00

(21)Application number : 11-296255
(22)Date of filing : 19.10.1999

(71)Applicant : HITACHI LTD
(72)Inventor : HIROSE TAKAHIRO
KAGIMASA TOYOHIKO
MAEOKA ATSUSHI

(54) CARD MONITORING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To cope with the progress and diversification of illegal access means.
SOLUTION: An IC card is equipped with a monitor program updating device. A monitor program is loaded from an external terminal device and arranged on a rewritable nonvolatile memory. When a new illegal access means is developed, the monitor program is updated to detect illegal access.



LEGAL STATUS

[Date of request for examination] 26.12.2002
[Date of sending the examiner s decision of rejection] 07.03.2006
[Kind of final disposal of application other than the examiner s decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner s decision of rejection]
[Date of requesting appeal against examiner s decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（JP）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2001－118042
（P2001－118042A）
(43)公開日　平成13年4月27日(2001.4.27)

(51)Int.Cl.[7]	識別記号	FI		テーマコード（参考）
G06K 19/073		G06F 12/14	320A	5B017
G06F 12/14	320	G06K 17/00	E	5B035
G06K 17/00		19/00	P	5B058

審査請求　未請求　請求項の数15　OL　（全 10 頁）

(21)出願番号　特願平11－296255

(22)出願日　平成11年10月19日(1999.10.19)

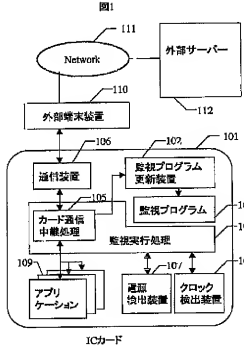
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　廣瀬　雅裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　鍵政　豊彦
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　カード監視方法

(57)【要約】
【課題】不正アクセス手段の進歩及び多様化に対抗する。
【解決手段】ICカードに監視プログラム更新装置を備え、外部端末装置から監視プログラムをロードし、書き換え可能な不揮発メモリ上に配置する。新手の不正アクセス手段が開発されたら、監視プログラムを更新することにより、不正アクセスを検出できるようにする。

図1



【特許請求の範囲】
【請求項１】ICカードシステムにおいて、外部からの不正なアクセスを監視するプログラムを書き換え可能なメモリ上に配置し、監視方法の変更に応じて前記プログラムを書き換えることを特徴とするカード監視方法。
【請求項２】請求項１記載のICカードシステムにおいて、カードの監視を実行する仮想計算機とカード監視プログラムを更新する装置を備え、安全に監視プログラムの更新及び実行することを特徴とするカード監視方法。
【請求項３】請求項２記載の方法において、すべてのアプリケーションに対する通信を監視することを特徴とするカード監視方法。
【請求項４】請求項２記載の方法において、不正なアクセスを監視するプログラム内に不正暗証番号として頻繁に利用される数字を格納しておき、外部端末より入力された暗証番号として比較することにより、不正なアクセスを検出することを特徴とするカード監視方法。
【請求項５】請求項４記載の方法において、ユーザに固有な数字を不正暗証番号リストとして利用することを特徴とするカード監視方法。
【請求項６】請求項４記載の方法において、カード所有者の個人情報に含まれる数字の一部又は全部を不正暗証番号リストとして利用することを特徴とするカード監視方法。
【請求項７】請求項２記載の方法において、カードシステムの消費電流又は消費電力を調べ、システムの動作を推定しうる変動パターンが現れていないか監視し、現れた場合は対抗手段を実行することを特徴とするカード監視方法。
【請求項８】請求項７記載の方法において、システムの動作を推定しうる変動パターンが現れた場合、動作中のアプリケーションの処理を強制的に中断することを特徴とするカード監視方法。
【請求項９】請求項８記載の方法において、動作中のアプリケーションの処理を強制的に中断させた後、当該アプリケーションを使用不能に設定することを特徴とするカード監視方法。
【請求項１０】請求項７記載の方法において、システムの動作を推定しうる変動パターンが現れた場合、無意味な処理を行い消費電力及び消費電流を均一化する処理を起動することにより、システムの挙動を隠蔽することを特徴とするカード監視方法。
【請求項１１】請求項３記載の方法において、不正アクセスに頻繁に利用されるバイト列を格納しておき、通信データ中に当該バイト列が現れた場合、対抗手段を実行することを特徴とするカード監視方法。
【請求項１２】請求項１記載の方法において、アプリケーションの更新処理と監視プログラムの更新処理を分離し、監視プログラムの更新処理においては、アプリケーションの更新処理よりも長い鍵又は強度の高い暗号アルゴリズムを用いることを特徴とするカード監視方法。
【請求項１３】請求項１記載の方法において、監視プログラム更新時に、ICカード上に存在する監視プログラムと最新版監視プログラムの差分のみをカードに送信することを特徴とするカード監視方法。
【請求項１４】請求項１記載の方法において、ICカードからサーバに、監視プログラムのバージョン情報を暗号化して送信することを特徴とするカード監視方法。
【請求項１５】請求項１記載の方法において、ICカードの起動時に、通常のアプリケーションの処理に先立って、監視プログラムの更新処理を行うことを特徴とするカード監視方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】ICカード利用において、不正利用を防ぐ技術に関する。
【０００２】
【従来の技術】ICカードは外部からの不正アクセスを検出するために、様々な監視を行っている。例えば、暗証番号の入力を監視する。特開昭62-190585と特開昭62-280965は、暗証番号の照会の不一致回数に上限を設定し、暗証番号の推測による不正なアクセスからカードシステムを保護する。特開昭60-181888は、ICカードに暗号を格納しておき、端末装置から送られてくる暗号と一致するか調べることにより不正なアクセスを防いでいる。
【０００３】
【発明が解決しようとする課題】技術の進歩と共に、不正アクセスの技術も進歩している。新手の不正アクセス技術が開発されると、旧来の監視システムでは、不正アクセスを検知できない恐れがある。短い周期でカードを更新していけば対抗できるが、コストがかさむ上、ユーザーにとっても不便である。
【０００４】また、マルチアプリケーションカードの場合、カードにロードされているアプリケーションの種類によって監視すべき項目が違ってくる。カードの出荷時に最適な監視項目を決めることが困難である。
【０００５】
【課題を解決するための手段】ICカードシステムにおいて、監視プログラムをサーバから動的にダウンロードできるようにし、外部からの不正なアクセスを監視するプログラムを書き換え可能なメモリ上に配置し、監視方法の変更に応じてプログラムを書き換える。
【０００６】
【発明の実施の形態】図1は全体の構成を示している。ICカード101は外部端末装置110を介して外部のネットワーク111上のサーバ112と通信を行う。ICカード101内には、通信装置106、監視プログラム更新装置102、監視実行処理103、電源検出装置107、クロック検出装置108がある。これらの装置は、ハードウエア又はROM上のソフトウエアによって実装する。アプリケーション109と監

視プログラム104は、書き換え可能な不揮発メモリに実装する。アプリケーション109と監視プログラム104のうち、変更する必要性のない部分はROM上に実装しても良い。通信装置106は外部端末110との物理的接点を持ち、カード外部との通信を行う。監視実行処理103内のカード通信中継処理105は、通信装置106、監視プログラム更新装置102、アプリケーション109の間で、通信データの配送を行う。監視プログラム更新装置102は、外部（サーバ112）からネットワーク111を介して監視プログラム104をロードしてカード内不揮発メモリ上に配置する。監視実行処理103は、監視プログラム104を実行する仮想計算機であり、ソフトウエアで実装してある。監視プログラム104は、監視実行処理103上でカード稼動状況を監視し、不正なアクセスを検出するプログラムである。電源検出装置107は、電源電流と電源電圧の変動パターンを監視実行処理103に提供する。クロック検出装置108は、クロックの変動状況を監視実行処理103に提供する。

【０００７】図2は、カード監視システムのチップ上の配置を示している。カードシステムは1チップのマイコン201上に実装する。マイコンチップ201上には、CPUコア領域202、RAM領域203、周辺回路領域204、読み出し専用不揮発メモリ領域205、書き換え可能不揮発メモリ領域206があり、これらは、内部バス210を介して互いに接続されている。これらはいくつかのブロックに分けて実装されることもある。CPUコア領域202は、メモリに格納された命令を実行し、マイコンチップ全体を制御する。RAM領域203は、CPUコア202が命令実行するための一時的なデータ格納領域である。周辺回路204がその一部を一時記憶領域として利用することもある。周辺回路領域204には、CPUコア202に含まれない様々な処理を行う回路が収められている。例えば、チップと外界とのデータ交換を行う通信装置106、電源検出装置107、クロック検出装置108、などが含まれる。読み出し専用不揮発メモリ領域205には、カードOS207、周辺ドライバ208、監視プログラム更新処理102、監視実行処理103が格納される。書き換え可能不揮発メモリ領域206には、監視プログラム104とアプリケーション109が格納される。書き換え可能不揮発メモリ206は、EEPROM、Flashメモリ、強誘電体メモリ等である。なお監視プログラム104のうち、変更する必要のない部分は、読み出し専用不揮発メモリ205に格納しても良い。

【０００８】図3は、監視実行処理103の構成を示している。監視実行処理103はソフトウエアで実装した仮想計算機である。仮想計算機内では、監視プログラム104の挙動をモニターしていて、監視プログラム104が不正にアクセスしようとしても、仮想計算機がこれを検出して例外信号を発生させる。仮想計算機内には大きく分けて、スタック301、プログラムカウンタ(PC)302、オブジェクト領域303、監視プログラム格納領域304の4つの構成単位よりなる。スタック301は演算の途中結果を保持する一時記憶領域である。プログラムカウンタ302は実行中の仮想命令のアドレスを保持する記憶領域である。監視プログラム格納領域304は監視プログラム104の仮想コードを保持する領域であり、通常書き換え可能な不揮発メモリ206上に置く。オブジェクト領域303は、監視プログラム104の実行に必要なオブジェクトを格納する領域である。オブジェクトは、監視実行処理組み込みオブジェクトと監視プログラムオブジェクトに分けられる。監視実行処理組み込みオブジェクトは、監視プログラムがICカード内の各装置にアクセスするためのインターフェースの役割を果たすオブジェクトである。通常、ROM上に格納され、ICカードが初期化されてから破棄されるまで存在し続ける。図中では、例として通信オブジェクト305、電源オブジェクト306、クロックオブジェクト307を示してある。通信オブジェクト305は、監視実行処理103がカード通信中継処理105を実行するときに使用する。電源オブジェクト306は、監視プログラムが電源検出装置１０７にアクセスするときに使用する。クロックオブジェクト３０７は、クロック検出装置108にアクセスするときに使用する。監視プログラムオブジェクトは、監視プログラムが生成したオブジェクトである。通常、書き換え可能な不揮発メモリ上に格納され、生成した監視プログラムが削除されると、一緒に削除される。ただし、監視プログラムのバージョンアップの場合は、そのまま残す場合が多い。図中では、例として試行回数カウンターオブジェクト308と通信パターンオブジェクト309を示してある。試行回数カウンターオブジェクト308は、暗証番号の入力が一致しなかった回数を記録するオブジェクトである。通信パターンオブジェクト309は、不正な外部アクセスのパターンを記録したオブジェクトである。

【０００９】図4は、電源検出装置107の構成を示している。電源サンプル装置405は、電源サンプルタイマ404からの指示を受けて、電源の電圧値や電流値を取得する。取得したデータは、即座に電源データ蓄積装置403に転送される。電源サンプルタイマ404は、定期的に電源サンプル装置405にデータ取得指示を出す。電源サンプルタイマ404が指示を出す時間間隔は、固定にしても良いし、監視実行処理103からの指示で設定できるようにしても良い。電源データ蓄積装置403は、電源サンプル装置405から転送されてきたデータを蓄積し、ある程度まとまったところで、電源データ転送装置401に渡す。データを渡すタイミングは、データ転送タイマ402の指示に従う。データ転送タイマ402が指示を出す時間間隔は、固定にしても良いし、監視実行処理103からの指示で設定できるようにしても良い。電源データ転送装置401は、電源データ蓄積装置403から受け取ったデータを、監視実行処理103の受け付ける形式に変換して転送する。バイト列形式に変換すると、パターンマッチ処理で

電源データを検査することができる。

【0010】図5は、監視プログラム更新装置102の構成を表している。監視プログラム更新制御装置501は、更新処理の手順にしたがって各装置を起動し、更新処理全体の流れを制御する。監視プログラム認証処理502は、外部から転送されてきた監視プログラム104を調べて、正当な監視プログラムであることを認証する。監視プログラム認証処理502は、内部に認証鍵を格納したデータベース503を持っており、認証鍵データベース503から適切な鍵を選択して、その鍵を使って認証を行う。監視プログラム書き込み装置504は、認証した監視プログラムを、監視実行処理103内の監視プログラム格納領域304に書き込む。監視プログラム削除装置505は、監視実行処理103内の監視プログラム格納領域304から、不要になった監視プログラムを削除し、メモリスペースを解放する。

【0011】図6は、監視プログラム104の構成を示している。監視プログラムは、外部（サーバ112）からネットワーク111を介してロード可能なので、監視プログラムの中身はICカードによって異なる。ここでは監視プログラムの一例を挙げ、監視プログラムの動作を説明する。例の監視プログラム104は、通信データ、電源変動、クロック変動の3つの項目の監視を行い、不正なアクセスを検出する。通信監視モジュール601は、カード通信中継処理105から通信フレームを得て、外部から不正なアクセスがないかどうか監視する。通信監視モジュール601には通信パターンマッチング処理部602があり、ここで通信フレームの検査を行う。通信パターンマッチング部602は、内部に暗証番号データベース604と通信パターンデータベース603を持っている。暗証番号データベース604内には、不正暗証番号リスト605と試行回数カウンタ606がある。暗証番号データベース604は、暗証番号フレームの検査に使用するデータベースで、暗証番号以外のフレームは通信パターンデータベース603を使用する。検査手順の詳細は後述する。電源監視モジュール607は、電源の変動からアプリケーションの処理内容を見抜かれることのないようにするため、電源の変動を監視する。電源監視モジュール607内には、電流変動監視処理608と電圧変動処理611がある。電流変動監視処理608は、電流変動パターンデータベース603を参照しながら、電流の変動を監視し、直宣、電流変動均一化処理610を起動する。電流変動均一化処理610は、無意味な処理をアプリケーションと並行して動作させることで、消費電流の変動パターンを変え、消費電流からアプリケーションの挙動を推測できないようにする。クロック監視モジュール612は、クロック変動を監視し、極端に遅いクロックが入力されたり、処理中にクロックが許容値以上に変動した場合、不正アクセスが行われていると判断し、対抗手段を実行する。対抗手段としては、アプリケーションのブロック、カードのブロック、カードのリセット等の処理がある。

【0012】図7は、監視プログラム104のフォーマットを示している。先頭にはヘッダ701があり、プログラムのバージョンや提供者の情報が書いてある。監視プログラム認証署名情報702は、監視プログラムが正当なものであることを証明するための情報が入っている。通常、監視プログラム提供者の秘密鍵で暗号化した署名が入っている。監視プログラム仮想コード704は、監視実行処理が実行するプログラムのコードを格納している。オブジェクト初期化情報705は、監視プログラムを初期化する時に使用するデータを格納している。監視プログラム属性情報703には、プログラムのサイズや使用する資源等の情報が格納されている。

【0013】図8は、監視プログラム104を外部からロードして更新する処理の手順を示している。ステップ801で外部端末装置110との通信接続を確立する。ICカードと物理的な通信を行うのは、ICカード端末装置110である。論理的な通信相手は、ICカード端末である必要はなく、PCやネットワーク111上のサーバ112であっても良い。ステップ803で、外部端末装置から外部端末装置の正当性を証明する署名を送ってもらう。ステップ804で、認証鍵データベース503に格納してある鍵を使って署名を認証する。署名が正しければステップ805に処理を移す。署名が不正であれば、処理を終了するか、ICカードをブロックする等の対抗手段を実行する。図中では単純に処理を終了している。ステップ805で、監視プログラムを格納したファイルを受信する。ステップ806で、監視プログラムファイル中から署名702を取り出し、認証鍵データベース503の鍵を使って認証する（ステップ808）。正当な署名であれば、ステップ809からステップ810に処理を移す。不正な署名であれば、処理を終了するか、ICカードをブロックする等の対抗手段を実行する。図中では単純に処理を終了している。ステップ810で、監視プログラム書き込み装置504を起動し、監視プログラムのロード処理を開始する。ステップ811で、監視実行処理103内の監視プログラム格納領304域にアクセスし、必要な領域を確保する。ステップ812で、確保した領域に監視プログラム104を書き込む。この他に特定の初期化処理が必要であればそれを実行する。

【0014】図9は、通信監視モジュール601の処理手順を示している。ステップ901で、カード通信中継処理105から、受信したフレームを取り出す。ステップ902で、通信フレームを調べ、暗証番号フレームであれば、ステップ903に処理を移し、そうでなければ、ステップ905に処理を移す。ステップ903で、不正暗証番号リスト605と受信した暗証番号を比較する。不正暗証番号リスト605には、生年月日、電話番号、自動車登録番号のように、暗証番号の推測に良く使われる番号を格納している。ステップ904の比較で、これらと一致したら、不正なユーザーが暗証番号を推測していると判断し、ステップ907

に処理を移す。ステップ907で、該当するアプリケーションをブロックする、ICカードをブロックする、カードをリセットする、又はアプリケーションを異常終了させる等の対抗手段を実行する。通信パターンデータベース603には、不正アクセスで頻繁に利用されるバイト列を格納してある。ステップ905で比較を行い、通信フレーム中にこれらのバイト列が含まれていたら、不正なアクセスを受けている可能性が高いと判断し、ステップ906からステップ907に処理を移し、対抗手段を実行する。

【0015】図10は、電源監視モジュール607の処理手順を示している。ステップ1001で、電源検出装置107から電源電流の変動パターンを取得する。ステップ1002で、電源電流変動パターンデータベース609に登録されているパターンと比較する。ICカードシステムの消費電流を詳細に調べることで、アプリケーションの挙動を推測することができる。アプリケーションが不注意な処理を行うと、推測の手掛かりとなるような電流変動パターンが表れてしまうことがある。そのようなパターンが表れた場合は、ステップ1003からステップ1005に処理を移し、対抗手段を実行する。ここでは、ステップ1005で、電流変動均一化処理610を起動する。この他にアプリケーションを異常終了させたり、アプリケーションをブロックする等の対抗手段もある。電流変動均一化処理610は、無意味な処理を行い消費電流を変えるルーチンである。アプリケーションと並行して動作させることで、消費電流の変動パターンを変え、消費電流からアプリケーションの挙動を推測できないようにする。一致するパターンがない場合は、ステップ1004に処理を移し、電流変動均一処理610を停止する。電流変動均一化処理610は、ICカードの処理速度を下げたり、ICカードの消費電流を増やす副作用がある。危機が過ぎたら停止しても良い。特にセキュリティが重視される場合は、アプリケーションが終了するまで動かしておく方が良い。さらに高度なセキュリティを要求する場合は、常に起動しておくという方法もある。

【0016】図11は、外部カード端末装置110の内部構成を示している。端末装置110は、カード通信装置1101とネットワーク通信装置1102を備え、それぞれICカード及び外部ネットワークと通信を行う。これらの通信装置は、端末制御装置1103により制御されている。また端末制御装置1103は、カード識別処理部1104、監視プログラム更新処理部1105、端末側アプリケーション1106を起動及び制御する。カード識別処理部1104は、ICカードからの応答を受け取り、ICカードの種別を認識する。ICカードが監視プログラム更新機能を備えていると判断した場合は、監視プログラム更新処理部1105に制御を移し、更新処理を実行する。監視プログラム更新処理部1105は、ICカードとサーバの間の通信を確立し、監視プログラムの更新処理を行う。監視プログラム更新処理部1105自身が直接更新処理を行う訳ではなく、ICカードとサーバの間で実行される。監視プログラム更新処理部1105は、両者間のデータ変換を行い通信セッションを確立する。端末側アプリケーション1106は、カード側アプリケーションと連携して、アプリケーションを実行する。

【0017】図12は、外部カード端末装置110の処理手順を示している。ステップ1201で、端末制御装置1103は、ICカードが挿入されたことを認識すると、カード通信装置1101を起動し、ICカードの初期化を行う。ステップ1202で、端末制御装置1103は、カード通信装置1101を経由してICカードからカード種別情報を取得し、カード識別処理1104に転送する。ステップ1203で、カード識別処理部1104は、転送されてきた種別情報を調べ、監視プログラム更新機能を持ったICカードであるかどうか判断する。監視プログラム更新機能を持っていなければステップ1207に処理を移す。持っていればステップ1204に処理を移し、監視プログラム更新処理部1105を起動する。ステップ1204で、監視プログラム更新処理部1105は、端末制御装置1103経由でネットワーク通信装置1102にアクセスし、ネットワーク上の監視プログラム更新サーバ112を検索する。更新サーバ112が見つかったら接続を試みる。ステップ1205で、サーバ112に接続できたらステップ1206に処理を移し、接続できなかったらステップ1207に処理を移す。ステップ1206で、ICカード内の監視プログラム更新装置102を起動する。このときカード側が端末の認証を求めてくることがある。その時は端末の署名を送信し、ICカードに認証させる。ICカード側から要求が無ければ何もしなくて良い。以後は主にICカードとサーバの間で更新処理を進める。更新処理が終了したらステップ1207に処理を移す。ステップ1207は通常のICカード処理である。ユーザの指定又はデフォルト設定により適切なアプリケーションを起動し処理を行う。ここで示した手順では、通常のアプリケーションの処理に先立って自動的に監視プログラムの更新を行う。これによりユーザに意識させることなく、監視プログラムを常に最新版に維持することができる。この他に、ユーザの指示に基づいて監視プログラム更新装置102を起動して更新処理を実行させても良い。

【0018】図13は、外部監視プログラム更新サーバ112の構成を示している。更新サーバ112は、一般にネットワーク機能を持った汎用計算機上に構築する。データベース処理や暗号処理向けに専用ハードウエアを付加しても良い。ネットワーク通信装置1306は、ネットワークを経由してICカード及び端末装置と通信を行う。監視プログラム更新制御部1301は、監視プログラムの更新処理全体を制御する。暗号化復号化処理1302は、監視プログラムの署名付け、暗号化、及びバージョン情報（後述）の復号化等の処理を行う。更新サーバ112は、処理に必要なデータを保持するため、カード情報データベース1303、監視プログラムデータベース1304、暗号鍵データベース1305を持っている。カード情報データベース1303

は、カード種別、カード番号、OSのバージョン、監視プログラム更新装置102のバージョン等の情報を保持している。監視プログラムデータベース1304は、監視プログラムのバージョン情報と監視プログラムそのものを格納している。監視プログラムは索引付けされており、ICカードに適した監視プログラムを迅速に取り出せるようになっている。暗号鍵データベース1305は、監視プログラムの署名付け暗号化、バージョン情報の復号化、ICカードの認証等に使用する暗号鍵を格納している。

【００１９】図14は、外部監視プログラム更新サーバ112の処理手順を示している。サーバー上の更新プロセスは、通常、ICカード及び端末装置からの要求により処理を開始する。ステップ1401で、要求してきたカードに対してバージョン取得コマンドを送信する。バージョン取得コマンドとは、ICカードに対して現在稼動している監視プログラム104のバージョンの情報取得を要求するものである。このコマンドは暗号化して送信しても、平文で送信しても良い。ステップ1402で、ICカードからバージョン情報を受信する。監視プログラム104のバージョン情報は、暗号化して更新サーバー112に送信される。監視プログラム104のバージョンが判ってしまうと、不正を行う者に情報を与えてしまうことになる。暗号化することで監視プログラムのバージョンが漏洩することを防ぐ。ステップ1403で、カード情報データベース1303と暗号鍵データベース1305を参照して、適切な暗号鍵を選び出し、バージョン情報を復号化する。ステップ1404で、監視プログラムデータベース1304を参照し、ICカード上の監視プログラム104が最新版であるかどうか検査する。最新版であれば処理を終了する。最新版でなければステップ1405に処理を移す。ステップ1405で、ICカードが正当なものであることを確認するため、認証要求を送信する。ステップ1406で、ICカードから返送されてきた署名を認証する。なお、認証署名は、ステップ1402のバージョン情報と一緒に送っても良い。この場合、ステップ1405とステップ1406は、ステップ1403の処理に統合される。その結果、ICカードとサーバの通信回数が減るので、多少効率が良くなる。ステップ1407で、カード情報データベース1303と暗号鍵データベース1304を参照して、ICカードに適した暗号鍵を選択する。監視プログラムの更新に使用する暗号鍵は、アプリケーションの更新に使用する鍵とは別の鍵を使用する。通常、アプリケーションの更新鍵より長い鍵を使用し、監視プログラムが不正に更新されないように保護する。アプリケーションの更新よりも機密度の高い暗号アルゴリズムを用いても良い。ステップ1408で、監視プログラムデータベース1304から最新版の監視プログラムを取り出し、先に選択した暗号鍵で署名及び暗号化する。監視プログラム全体を暗号化する代りに、ICカード上の監視プログラム同一バージョンの監視プログラムと最新版の監視プログラムとの差分を取って暗号化しても良い。ICカードには差分のみを送信し、ICカード内で最新版の監視プログラムを再構成する。これにより通信量を削減することができる。最後にステップ1408で、暗号化した監視プログラムをICカードに送信する。

【００２０】

【発明の効果】本発明によれば、監視プログラムを、新手の不正アクセスを検出可能な最新版に更新することで、不正アクセスを検出しICカードを保護することができる。

【図面の簡単な説明】

【図１】カード監視システムの全体構成である。

【図２】カード実レシステムのチップ上の配置である。

【図３】監視実行処理の構成である。

【図４】電源検出装置の構成である。

【図５】監視プログラム更新装置の構成である。

【図６】監視プログラムの構成の例である。

【図７】監視プログラムのファイル形式である。

【図８】監視プログラムのロード手順である。

【図９】カード通信の監視手順である。

【図１０】カード電源の監視手順である。

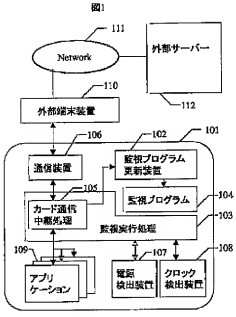
【図１１】外部端末装置の構成である。

【図１２】外部端末装置の処理手順である。

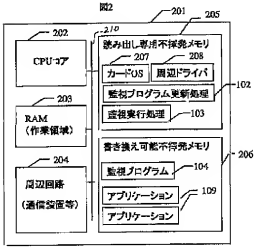
【図１３】外部監視プログラム更新サーバの構成である。

【図１４】外部監視プログラム更新サーバの処理手順である。

【図1】

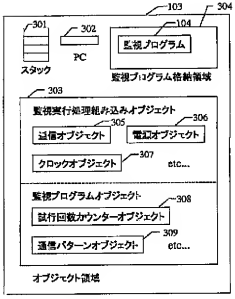


【図2】



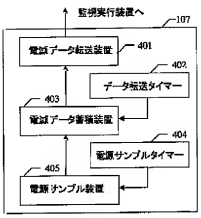
チップ上のシステムの構成

【図3】



監視実行処理

【図4】



電源検出装置の構成

【図5】

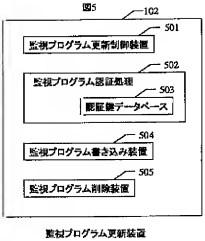


図5
102
501
監視プログラム更新制御装置
502
監視プログラム認証処理
503
認証鍵データベース
504
監視プログラム書き込み装置
505
監視プログラム削除装置
監視プログラム更新装置

【図6】

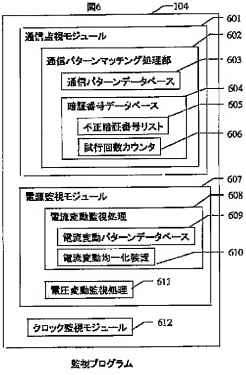


図6
104
601
通信監視モジュール
602
通信パターンマッチング処理部
603
通信パターンデータベース
604
暗証番号データベース
605
不正暗証番号リスト
606
試行回数カウンタ
607
電源監視モジュール
608
電流変動監視処理
609
電流変動パターンデータベース
610
電流変動均一化装置
611
電圧変動監視処理
612
クロック監視モジュール
監視プログラム

【図7】

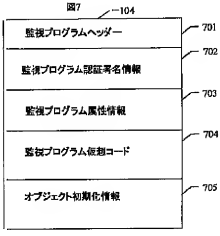


図7
104
701
監視プログラムヘッダー
702
監視プログラム認証署名情報
703
監視プログラム属性情報
704
監視プログラム仮想コード
705
オブジェクト初期化情報

【図8】

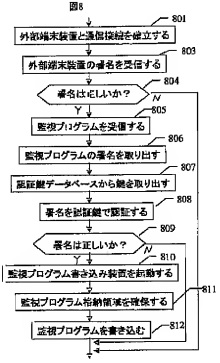
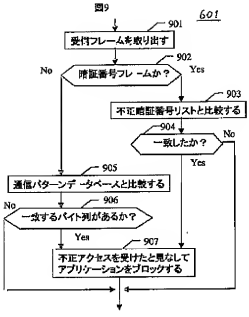
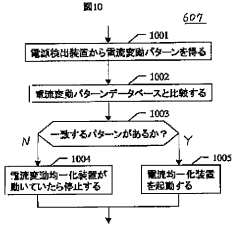


図8
801
外部端末装置と通信接続を確立する
803
外部端末装置の署名を受信する
804
署名は正しいか？
N
Y
805
監視プログラムを受信する
806
監視プログラムの署名を取り出す
807
認証鍵データベースから鍵を取り出す
808
署名を認証鍵で認証する
809
署名は正しいか？
N
Y
810
監視プログラム書き込み装置を起動する
811
監視プログラム格納領域を確保する
812
監視プログラムを書き込む

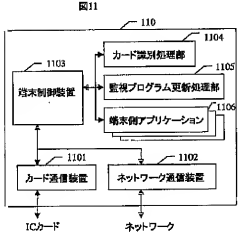
【図９】



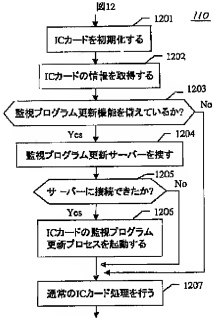
【図１０】



【図１１】

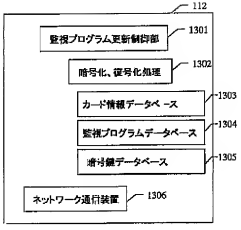


【図１２】



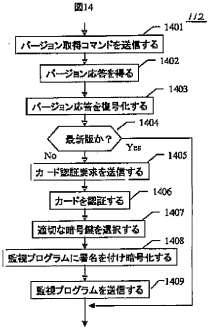
【図13】

図13



【図14】

図14



フロントページの続き

(72)発明者　前岡　淳
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Fターム(参考)　5B017 AA08 BA08 CA14
5B035 AA13 BB09 CA38
5B058 CA27 KA31